AU00/251

4

09/937961

Patent Office
Canberra

I, LEANNE MYNOTT, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PP9477 for a patent by LISA HORTEN AND ELIK SZEWACH filed on 29 March 1999.

WITNESS my hand this
Seventh day of April 2000

LEANNE MYNOTT
TEAM LEADER EXAMINATION
SUPPORT AND SALES

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

ORIGINAL

AUSTRALIA

Patents Act 1990

PROVISIONAL PATENT SPECIFICATION

APPLICANT: Lisa HORTEN and Elik SZEWACH

ADDRESS: both of 8/26 Eumeralla Road Caulfield South, Victoria ??

INVENTORS: Lisa HORTEN, Elik SZEWACH and Ian DONALD

ADDRESS FOR SERVICE: Paul A Grant and Associates PO Box 60, Fisher, ACT, 2611

INVENTION TITLE: Remote Live Gaming System

The invention is described in the following statement:–

TITLE: REMOTE LIVE GAMING SYSTEM

TECHNICAL FIELD

This invention relates to gaming systems, methods and means where a game takes place between real people in real time via telecommunication links that include live video, and where money or credit transfers take place in as the game progresses. The live video link in such systems may be used to show the players to one another or to merely show a croupier and gaming table to remote players.

Since aspects of the invention relating to the systems security of financial transactions conducted over a telecommunications or computer network are applicable elsewhere than in gaming, this invention also relates to methods for effecting computer-systems security and to such computer systems.

BACKGROUND TO THE INVENTION

Many casinos seek to attract premium or VIP players (herein called 'high-rollers') to their tables, but gamblers who play for high stakes generally like to participate in games involving other high-rollers and casinos cannot always arrange for such players to be present at one time. Also, many high-rollers are busy people who cannot afford the time to travel to a casino – whether in their own country or another – for the sake of one or two games. It would be desirable, therefore, to have a gaming system that allows gamblers at one or more remote locations to participate in a casino game, perhaps involving a dealer or croupier and perhaps including one or more other players at a casino table, in a realistic manner. It may also be desirable in such games to allow the players to be anonymous (with respect to one another, if not the casino), should they so desire. In any such system, however, it would be essential to ensure a high level of security in relation to the financial transactions of both the casino and the player, to safeguard the privacy of the remote player (to the degree required by the player), and to minimise the opportunity for fraud on the casino, the players or their respective banks.

In addition it would be desirable for the game to be played as realistically as possible (subject to the degree to which the identity of the players is revealed).

Thus, it would be desirable for all players to see the croupier and the table or wheel, to hear any calls or comments by the croupier, to observe the cards or dice as they fall, to be able to cut a deck of cards as required, to see cards discarded or laid face-up by the croupier or other players, etc. In addition, it would be desirable for each remote player to have a supplementary visual display showing his/her hand, the bets as they are placed and as they stand, the numerical results of a throw of dice or spin of the wheel, who's turn it is to place a bet, who has passed, a textual presentation (in the player's preferred language) of any calls by the croupier, etc.

It is well known to facilitate multi-player gaming on a network such as the Internet where a server runs a master video game program, accepts moves from gamers and re-computes the game situation in an interactive fashion. US patent No. 5,630,757 to Gagin discloses a system of this type that employs a multi-threaded, multi-process computer operating system and a special protocol for communication via cable TV channels. Multi-player video gaming is also known where each player employs a copy of the game program on his/her PC and connects to the Internet to interact with other players. In these systems the players can remain anonymous (if desired) and live video is not an option. Such systems are not suitable for croupier-mediated interactive live gambling, nor do they allow for betting and the on-line payment of wins and losses.

It is has also been proposed to use 'electronic playing cards' in casino-mediated poker and the like games to eliminate the danger of card marking and 'cross-roading' (improper manipulation by a croupier to favour or disfavour a particular player). For example US patent No. 5,669,817 discloses the use of computer monitors for each player and for the dealer so that cards can be dealt electronically and each player's hand can be displayed to him/her alone. While 'electronic' shuffling, cutting and dealing has the advantage of avoiding croupier bias, the system of the last mentioned US patent required the croupier and players to be in the same room and all losses and wins to be settled on-site in the normal manner. No means of enabling remote play via live video, or remote settlement, was disclosed.

The participation of multiple remote players in a common board game via a network is also known. For example, US patent No. 4,372,558 discloses means whereby two remote Go players can each make physical moves (in proper sequence) on their individual boards and have the moves validated and transmitted for display to the other player. In this case, however, live interactive video and audio links are not used and no provision is made for gambling or the handling of financial transactions.

US patent No. 5,762,552 to Vuong et al discloses an interactive real-time gaming system that has provision for both audio and visual feeds and allows players at remote audio-visual terminals to place bets in more than one casino-operated game of chance at one time. However, the system is such that the remote bets must be placed at rates that are independent of rates of play of each game. This greatly limits the type of game that can be played using the system. Of most importance in the context of the present invention many – if not all – live, croupier-mediated casino games of interest to high-rollers will be excluded. In fact, the non-synchronous play feature effectively confines the system to paying multiple slot machines or other machine-generated games of chance where bets can be 'stacked' in advance of play. Though the need for financial security and authorisation is recognised by the teachings of this patent, there is no disclosure of a suitable method of implementing the necessary authorisation and security.

US patent No. 5,800,268 to Molnick discloses a method of validating the financial transactions of players who participate in a live casino game from remote locations via a communications network. Each remote player receives live television and data signals relating to a casino game at his/her remote station and uses it to convey bet information to the casino. Before the player is permitted to join a game or place a bet, the casino establishes a direct and open link to the player's bank or other financial institution that allows the casino to instantaneously (i) check that the player has enough credit to cover each bet as it is placed (ii) pay winnings directly into the player's account and (iii) recover losses directly from the player's account. The need to establish and keep open a line to each player's bank comprises considerable risk of fraud or misappropriation of that player's funds by casino employees, not to mention the loss of personal and (normally)

confidential financial information belonging to the player. Even when there is no foul play on the part of the casino or its employees who are privy to the player's personal and bank account details, the personal information gained by the casino is of great value in targeting further gaming products and in selling-off such information to direct-marketing agencies.

OBJECTIVE OF THE INVENTION

It is the objective of the present invention to provide an improved real-time interactive gaming system that will allow a remote player to participate in a realistic manner in a casino-mediated gambling game without unduly compromising the player's financial security, while allowing immediate real-time settlement of losses or wins on a game by game basis.

OUTLINE OF THE INVENTION

From one aspect, the present invention is based on the realisation that a remote player can electronically place money in a secure electronic purse for – and even during – each game so that the purse is accessible by the casino for (i) paying losses and wins and (ii) for checking the player's ability to cover any debit placed during a game. The use of such a purse avoids any access by the casino to the player's bank and, in accordance with preferred options, can allow a player to remain anonymous, once the validity of the purse has been confirmed by the casino.

In one possible mode of play, all the contents of each player purse may be transferred to a casino game purse – hereinafter called a 'safe' – and held in trust by the casino for the duration of the game. This would prevent a player from reneging on his/her gambling debts to the casino or other players by, for example, refusing to transfer the funds from his/her game purse, or switching off the player station when a debt was to be paid. Of course, during the course of each game, each player has (or can instantaneously access) a record of the amount of money 'in' his/her game purse, as well as records of the relevant transactions. At the end of each game, all wins and losses can be settled and the casino can transfer the appropriate monies to each player's purse. At that point, a player could transfer the cash in the purse back to his/her bank account or leave it in the purse pending

further gaming. Such an arrangement facilitates pari-mutuel gaming systems, which are mandated in some jurisdictions. A pari-mutuel system is one where the casino simply takes an agreed percentage of the player's stakes or transactions, leaving the wins and losses to be apportioned between the players; that is, it is not possible to bet against the casino in pari-mutuel gaming.

Preferably, the player's game purse comprises a smart-card that has been loaded with cash and where valid possession of the card has been verified by security means including biometric identification. Generally, it is preferable that the casino game purse should not be a smart-card but, rather, a secure computer file in the casino station. The safe storage of a number of smart cards by the casino is likely to present more security difficulties than a computer file. It is, however, envisaged that payments from the casino game purse will be authorised by the biometric identification of the croupier, or the biometric identification of a games supervisor who then checks the recommendations of each croupier and effects the funds transfer.

Conveniently, the player (smart-card owner) is provided with a personal EFTPOS terminal by his/her bank and employs it to transfer money from his/her bank account directly into the smart-card. This may be done via a bank-issued magnetic-stripe card and the appropriate PINs, via a separate smart-card owned by the player using PINs or biometric identification, or via the player's gaming smart-card itself. In this way, the bank-related transactions are kept private and secure with respect to the casino staff and other players. The casino must, however, be able to verify (i) that the gaming smart-card has been properly validated and (ii) the amount of money in that smart-card.

Biometric identification may be used only once at the start of a game and the establishment of the game-purse, or it may be used (at the player's option) to authenticate the placement of each bet. However, it is envisaged that, once a player and his/her station have been duly identified to the casino and once a game-purse has been established, the game can proceed (at the player's option) without further use of biometric identification or the player's personal security codes (eg, PINs). This allows a player to permit someone else to actually play a

game after it has been properly initiated until, if desired, the entire purse has expended. Unlike, the prior art system of Molnick, this can be done without providing the substitute player access to the authenticated player's bank account or PINs.

The particular biometric identification system or systems employed for the gaming smart-card will generally be determined by the casino, while that required for the banking smart-card will normally be determined by the bank. Known and commercially available biometric identification systems may be used. They include systems based upon fingerprint, voiceprint, iris and facial recognition.

From another aspect, the invention comprises a gaming system having a central (normally casino-based) croupier station and at least one remote player station including an electronic purse or cash-store, wherein one or more of the following security violations are alarmed and/or effect system and/or station shut-down or lockout:

- Any unauthorised substitution or modification of player station hardware or firmware (eg, EPROM or BIOS chips) during or prior to a game,
- Any attempt to access, read or change system files in the remote player station,
- Any unauthorised substitution or modification of croupier station hardware or firmware during or prior to a game,
- Any unauthorised attempt to access read or change system files in the croupier station, including files containing player details and including files and processes relating to the transfer of funds from players' purses.

Preferably, the security on the player's station is such as to allow the player to provide or change his/her own monitor (visual display device) and/or video recorder without causing system violation. In this way, a complete game with the play and all bets can be recorded and replayed by the player without also recording the data transferred between the casino and the player during a game. Of course, a record can also be made of accounting data provided by the casino with regard to the funds in the player's game-purse.

To implement these security provisions in respect of a player station normally requires that each player station be set up and supplied by the casino or system provider. This will generally rule-out the use of a regular PC by the player, though that is still possible if the PC is loaded with the necessary safeguards by the system-provider and appropriately sealed. Implementation of the security provisions in respect of the casino station will include similar hardware and software safeguards but will also include procedural safeguards for authorising and effecting (i) the loading of and access to player information and (ii) the transfer of cash to and from the player.

As is normal in data communication systems involving financial transactions, the data transferred between the player's smart-card reader and his/her station, as well as the data transferred between the croupier station and the player station, will be encrypted so that any eavesdropper will be unable to interpret that data. As already indicated, any unauthorised attempt to access encryption keys stored in either station will involve violation of station/system integrity and will cause system failure or player lock-out. Preferably, any such violation will leave an 'audit trail' in the respective station.

While encryption of video signals between the croupier and player stations is also desirable, it is not so important as encryption of the financial transactions. Preferably, a private ISDN system is employed wherein each station includes an ISDN terminal and wherein an ISDN bridge (located at the casino or in the premises of the telco) is employed to interconnect the casino and a plurality of player stations. The telecommunications media employed is unimportant as far as the present invention is concerned, it being left to the telco to furnish the necessary physical connections and bandwidth. It might be expected that optical fibre and microwave/satellite trunks would be employed and that ISDN connections would exist at each player's premises as well as at the casino.

DESCRIPTION OF EXAMPLES

Having generally portrayed the nature of the present invention, a particular example will now be described by way of example and illustration only. In the following description reference will be made to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of the system of the chosen example.

Figure 2 is a chart indicating the sequence of interactions between the player and casino stations during a typical gaming session employed in the system of the chosen example.

With reference to Figure 1, the general system 10 of the example comprises a central casino station 12 and two player stations 14a and 14b. In this example, casino station 12 comprises two gaming rooms 16a and 16b, each fitted with (i) a video camera [18a and 18b, respectively], (ii) a PC terminal [20a and 20b respectively] and a gaming table attended by a croupier [not shown]. Casino station 12 also includes a file server 22 and an ISDN video bridge 24, server 22 being connected to PC terminals 20 and to feed both data and control signals to bridge 24.

Bridge 24 includes an ISDN modem and video codec. It outputs data and video signals in ISDN format to a telecommunications carrier having ground transmit/receive dishes 26 and 28 and a satellite repeater 30. It will be appreciated that the telecommunications link might just as easily be terrestrial, or a combination of terrestrial and satellite links. The nature of this link is immaterial to the present invention. For convenience of illustration, player stations 14a and 14b are shown as each being connected to ISDN line 32 from common dish 28, but it will be appreciated that these stations may be in different countries and connected to different dishes or other telecommunication links.

Each player station 14 of this example comprises an ISDN interface unit 40 which includes an ISDN modem and video codec and which is connected to a dedicated PC 42 and to a video camera 44 which, at the option of the player(s) may be turned on or off during a game. PC 42 is preferably fitted with a touch screen and

is connected via data lines to (i) a smart-card writer/reader unit 45 and (ii) a personal EFTPOS terminal 46 that incorporates a modem, a telephone, a keypad and a swipe-slot for use with conventional magnetic stripe credit cards. If desired by the individual user, a large external display monitor, a video recorder and/or a printer may be connected to PC 42 by the player, but these items are not shown in the drawings.

Smart-card unit 45 is equipped with a biometric identification system (not separately illustrated) which, conveniently, includes a fingerprint recognising element. The biometric system might also or alternatively comprise an iris or face scanner and can comprise a separate unit that is connected direct to PC 42. These security devices are commercially available. For example, Seimens markets a smart-card as well as a smart-card reader capable of recognising the thumb-print of the owner. EFTPOS terminal 46 allows the player to dial his/her bank 48 via the POTS (plain old telephone system) lines 50 to effect the loading of a smart-card with cash (in a manner to be describe below) to establish a game purse. As a matter of convenience, the player stations 14a and 14b are assumed to be identical but their respective elements are distinguished from one another by the use of suffixes 'a' and 'b' respectively.

In normal use, the gaming system is employed and operated as will now be described. The casino sets up its central station and supplies player stations on lease or loan to selected patrons in remote locations. Each player station is installed by an employee of the casino in the premises of the player, or in the premises of an agent so that the one player station can be used separately by more than one player. The prime function of the casino employee is to separately register each intending player with the station, using a proprietary program supplied by the casino. This involves employing the biometric device to record one or more physical features of the player in the player station; for example, the player's thumbprint, facial dimensions, voiceprint and/or iris pattern. Some characteristic of each player's credit card can also be encoded by swiping the credit card in the card reader of the personal EFTPOS terminal provided by the payer's bank. The casino employee may also perform a number of secondary tasks in setting up the player station, though such tasks can be performed by any

competent technician; for example, the connection of the local ISDN port and the set-up of a video conference session. Indeed, provided suitable ISDN ports have been installed, a player or casino agent might be permitted to move the station between locations without further assistance from the casino.

Generally, supply and installation of the player's personal EFTPOS terminal will be effected by arrangement between the player and his/her bank, though it is essential that the EFTPOS terminal of each player who will use a player station be available for connection and identification when the casino employee sets up that station. Where the player station is installed in an agent's premises for use by more than one player, it will be normal for each player to simply bring his/her smart-card with them. Alternatively, and less conveniently, each player might bring his/her EFTPOS terminal with him/her to initiate the game purse on-site, the terminal being removed by the player at the end of the game session.

Preferably, the smart-card used to establish a player's purse for each game is supplied by the casino and encrypted with identification code recognisable to the player station (after it has been set up). It is also preferable that the smart-card reader is supplied by the casino and is encrypted with an identification code such that it is recognised by the player station upon start-up and such that the station will not operate if that particular reader not present or has been opened or modified in any way. Finally, it is also preferable that the player's smart-card can only be used in readers for which he/she has been registered (including, of course, the reader/writer attached to the player station), and in no other reader/writer. Thus, to establish a purse for a game at the player's premises (rather than an agent's premises), the player will normally have both his/her smart-card reader and his/her personal EFTPOS terminal connected to his/her player-station. In addition the player will normally have his/her personal EFTPOS station connected to his/her bank via a telephone link established independently of the casino system. By using whatever security codes or procedures agreed between the player and the bank (and unknown by the casino), the player can effect the transfer of 'cash' from the bank to his/her smart-card. Of course, the smart-card cannot be used for this purpose unless it has first been correctly

identified to the player station and unless the player who owns the smart-card has also been correctly identified to the player station.

Once the all participating players for a particular game have been 'assembled' on-line by the casino, the players can decide whether they wish to be identified or remain anonymous. If they wish to be identified, they may then decide whether they also wish to be seen via a two-way video conference set-up. If so, each player then turns on the video camera fitted to his/her player station and the two-way video conference system is set-up. Prior to this, each player would have established his/her game purse and the amount he/she is prepared to wager (ie, the sum in the purse) would have been read by the casino system.

Usually, each player would have a large monitor dedicated to providing a view of the gaming table and croupier at the casino. If a two-way video conference system has been established, the monitor would normally display the other players in separate windows located around the gaming table so that their movements and expressions can be observed and their calls heard by all participants. If the players choose to be identified but not to activate the two-way video-conferencing facility, a still image of each player could be substituted for the live image. Players can be assigned their real names or pseudonyms for the purpose of the game. These names can then appear in the appropriate places around the table (as displayed on the video monitors) and used by the croupier in oral communication with the players.

While the croupier responsible for a particular game would act exactly like a one at a conventional casino table, it is preferable that the results of a card shuffle, card deal, throw of dice or spin of the wheel be determined electronically in a truly random manner. Thus, the cards dealt by the croupier in a card game, the fall of dice in craps, the lodgement of the ball in a roulette wheel etc, would be computer-generated and shown (as appropriate) in a window that appears in the video monitor at the appropriate time. Besides depicting face-up cards on the casino table via the video link, the casino station communicates to each player the cards dealt to him/her in a manner that is securely hidden from the croupier and other players alike. Similarly, each player station communicates to the casino

station the identity of any cards discarded or turned face-up by the respective player and the results of any dice throw relegated to the player. While the casino station could determine the result of a player's dice throw using its random number generator, it is psychologically preferable that the player's station generates uses its own random number generator to determine the cast of the dice.

As in a normal casino game, however, the croupier is responsible for the management of a game, recording bets, signifying which player has the call, and resolving disputes between the players. To enhance realism, the croupier may physically place piles of chips in each player's position or elsewhere on the gaming table to indicate the lie of bets at a given time, moving them around at the end of a round to show bets lost and won in the normal manner. The placing of bets would, of course, be communicated electronically by the players at their respective player stations to the casino/croupier. If desired, bets placed by players could be digitally incorporated into the display of the casino table as visual images of piles of chips. As it is unlikely that the monetary value of a pile of chips can be determined reliably from the monitor display at a player station, each player has the facility to interrogate the value of any bet and/or to have all bets on the table shown clearly in dollar terms on his/her monitor. Other, more general, features of a game may also be displayed upon request by a player. For example, the rules of a game, the casino 'take', whether the game is being played in pari-mutuel mode, etc.

Security Considerations

It is desirable that the gaming system of the chosen example be secure from fraud or manipulation by any of the parties involved:

(a) by any player on the casino or other players,

(b) by the casino on any player,

(c) by the croupier on the casino and/or a player,

(d) by an employee of the casino or a third party with access to the casino station,

(e) by a casino employee or a third party with access to a player station,

(f) by a player's bank on its customer-player and/or the casino,

(g) by a player on his/her bank, or

(h) by a third party on a player.

These possibilities will now be considered individually.

(a) Fraud by a Player on the Casino or other Players

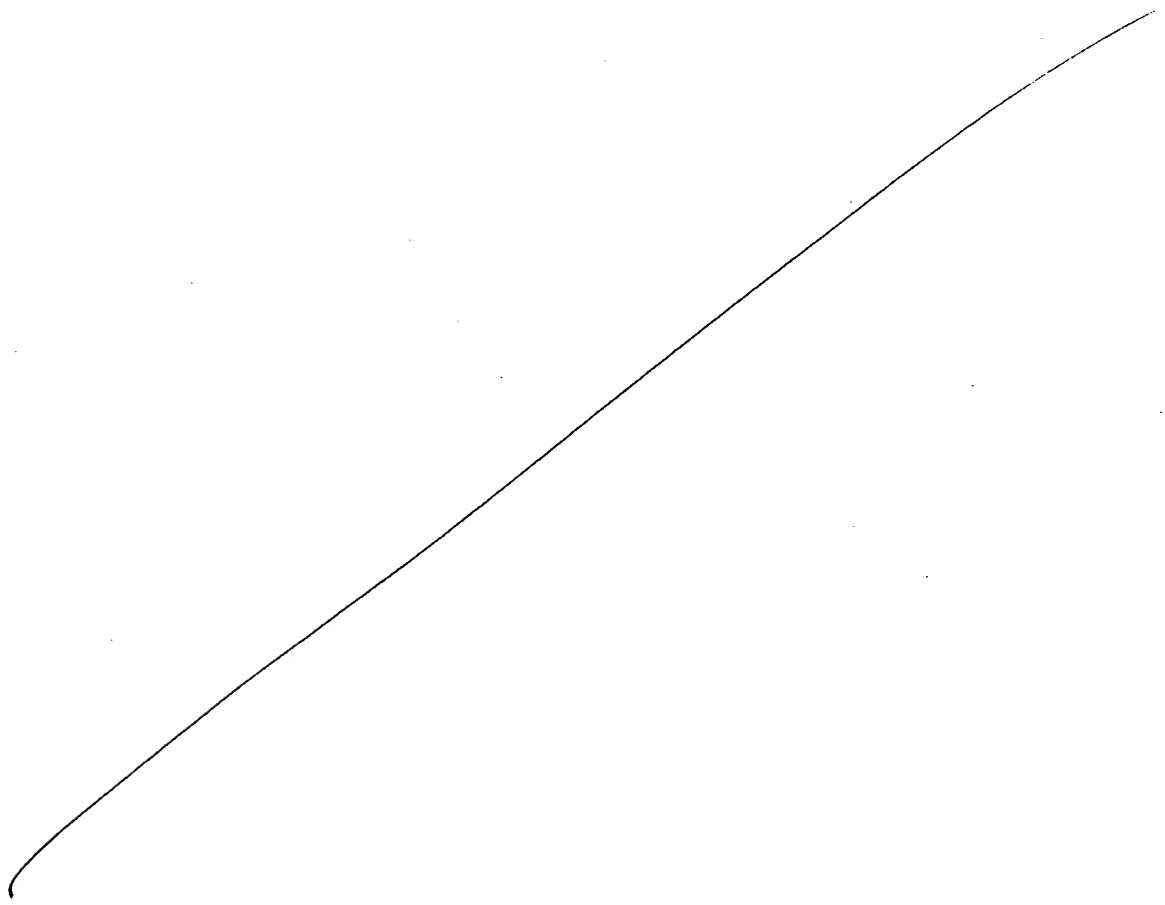
The principal and most serious avenues for a player to defraud the casino or another player are (i) to place bets that he/she cannot cover, (ii) to renege on a bet or play which has been made and (iii) to employ slight of hand to substitute cards or dice etc. These actions may be associated with the assumption of a false identity by the player concerned.

The first two avenues for fraud are closed off according to the present invention by the use of an open game-purse accessible and controllable (for the duration of a game) by the casino so that any player can be prevented from placing a bet which cannot be covered, from reneging on a bet which has been placed or from declining to pay a lost bet to the casino or another player. The third avenue for fraud is largely avoided by the use of electronic media and 'virtual' gaming where real cards and dice are not employed. The electronic equivalent of such fraud would be the programming of the player's machine to bias or determine the result of a throw of dice or a card deal or shuffle, or to change the cards dealt in a hand. These avenues for fraud are effectively prevented by securing the player's station against programming access or tampering.

(b) Fraud by the Casino on a Player

In any casino, the outcome of games and the odds in most games of chance can be manipulated – fraudulently or otherwise – by the casino management. This is so whether the games are played in-house or remotely, manually or 'computer-aided'. In essence, limitation or control of fraud by a casino on its clients is a matter for government regulation and policing. However, because statistics and recordings of all games played using the systems of this invention can be readily kept and analysed, systematic fraud on the part of the casino against its clients should be more easily detected using the gaming systems of the invention than otherwise.

That said, however, it is important to note that at least in one of the gaming systems envisaged by this invention, either the entire monetary amount in the purse of each player or a portion thereof is taken by the casino and held in trust in the casino's game purse during the course of a game. This procedure prevents a player from avoiding paying a loss by simply switching off his/her station when it is time to make payment. Of course, at the end of a game, the casino is expected to settle all wins and losses and to adjust all player purses accordingly. Nevertheless, this arrangement does enable the casino or someone with access to the casino station (typically a casino employee and, perhaps, the croupier) to rob the casino game purse and defraud the casino and/or the players. The effect of improper use of the game purse by the casino, one of its employees or a third party would be immediately detected at the end of a game by the players and legal redress would be available to the players if they were not compensated by the casino. Unauthorised access to the casino's game purse by an employee or a third party can be prevented by appropriate security procedures.



Fraud by the Croupier on the Casino and/or a Player

As already noted, the system of the present invention minimises the opportunity for croupier fraud because all dealing, roulette wheel operation and dice throwing can be effected electronically under computer control. Thus cross-roading (the selective favouring of one player with respect to another or with respect to the house) is effectively eliminated. This greatly lessens the current high cost of croupier supervision for a casino and relegates croupier bias to rulings on calls or conflicts between players – which is likely to be minimal because any (or every) player has the opportunity to record the game and analyse it at leisure. Further, since the croupier does not handle any money or 'real' chips, the opportunity for him/her to purloin some of the take by duping a player is also minimised.

Thus, the principal avenues for croupier fraud lie in (i) cross-roading where he/she misallocates payments from the casino purse between players, (ii) hacking of the casino purse program to allocate a portion of the casino or player's funds to another account, and (iii) hacking of the game program to change some feature to the advantage of himself/herself or that of one of the players. It would not be difficult for casino management procedures to effectively rule out croupier access to the system and, as will be explained below, the system itself can be made secure against unauthorised programming.

(c) Fraud by a Casino Employee (or another party) having Access to the Casino Station

As far as the gaming programs are concerned there are two problems here: the possibility of unauthorised access to the casino station, and the possibility of unauthorised changes to the system made by someone – normally a casino employee – having authorised access. The first threat can be rendered negligible by suitable internal security within the system itself (as will be described below), while the second can be avoided by have gaming programs written and checked by separate contractors, neither of whom are employees of the casino or have access to the system. Thus, there need be no provision in the casino station for access to the relevant programs or any means whereby they can be altered.

A more direct and serious threat of fraud lies in a the ability of a casino employee or third party to effectively gain access to the purses of the players – and/or to the casino game 'bank' – and to electronically transfer money therefrom to his/her own account. While this need not require any manipulation of the game, it does assume ability to 'hack the system' via the casino station, one or more player stations and/or the network generally. Again, protection against such fraud is a matter of inherent system integrity and security, a matter that is dealt with below.

(d) Fraud by a Player's bank on its Customer-Player and/or on the Casino

Though the ability and opportunities for a bank to defraud its customers are manifold, the risk of such fraud is not increased by the gaming system of the present invention. The opportunity and motivation for fraud are no greater than in normal electronic banking transactions involving credit cards and smart-cards, while the likelihood of detection and redress are no less. In any event, the proper transfer of funds between a player's bank and his/her smart-card need not be a function that is electronically mediated or controlled by the gaming system of the invention, being essentially a matter between the bank and the player. For that reason, the opportunity for a player's bank to defraud the casino appears negligible.

(e) Fraud by a Player on his/her Bank

As just noted, the transfer of funds between a bank and its customers is not a procedure that need be electronically controlled or mediated by the present gaming system. A bank is no more vulnerable to fraud by allowing a smart-card to be loaded with cash from one of its accounts for the purpose of gambling than for any other purpose. Whatever safeguards against fraud by its customers in such situations should prove adequate for the purpose of loading a smart-card for gaming purposes.

(f) Fraud by a Third party on a Player.

There are a number of opportunities for a third party to defraud a player, particularly if that party is trusted by or friendly with the player. First, such a person might be able to have his/her smart-card loaded from the player's bank. This danger is a matter for bank/player care and security attention, rather than the

system of the present invention. However, such fraud is rendered less likely by the present system in that biometric identification of the player can be required before the player's smart-card (and credit card, if desired) is accepted.

Second, the third party may have acquired the player's smart-card and wish to play a game without permission or knowledge of the player. This danger is avoided by the requirement that biometric identification of a player can be required at the start of each game. A further safeguard might be for the system to require each player to identify himself/herself biometrically immediately before any bet or play is made, though that could involve undesirable delays in game play.

As already noted under (d) above, a more direct and serious threat is one where a third party is able to hack into the gaming system while a game is in progress, gain access to a player's purse and electronically extract money therefrom. Access to the player's purse during a game may be pointless if the funds therein have been transferred to the casino and held in trust. In that case, fraudulent access to the player's card is limited to the times when it is still in place in a reader just before and just after a game. Protection against this threat relies upon ensuring system integrity and security.

Ensuring System Integrity and Security

The above analysis of the risk of fraud suggests that of primary concern is the protection of game-purse cash (both that of the casino and the players) against unauthorised access. Of secondary concern are (i) unauthorised modification of the random number generation and the card-shuffling routines in the casino and/or player stations to favour players against the casino or vice versa, and (ii), the hacking of transmissions between the players and the casino to alter bids or play.

Accordingly, data and video transmissions between the casino and each player are preferably encrypted using encryption keys located in both the player station and the casino station. Many commercial encryption systems are available of sufficient power to prevent eavesdropping by third parties on transmissions between the players and casino, and, to prevent effective signal substitution.

What is left, then, is the securing of the player and casino stations against unauthorised use, unauthorised access to the respective game purses and unauthorised access to the encryption keys.

The Player Station

In addition to safeguarding the encryption key and the player's game-purse, a player station needs to be secure against access by the player (or another person) to the random number generator used by the player to signify to the casino station the roll of dice or the cutting, shuffling and dealing of a pack of cards. To achieve the desired level of security, one or more of the following features may be incorporated in each player station:

1. No externally accessible disc drives or connections therefor are provided so that the only ways of changing settings within the station are (i) by physical substitution of station components (eg, plug-in cards or ROM chips) and (ii) via the network using encrypted commands.
2. The station is housed within a casing that is physically locked against opening and is alarmed so that, immediately the casing is opened, key data (eg the purse software, the BIOS, all encryption keys and important hard-disc files) is deleted or the unit is otherwise crippled.
3. All key components of the player station, including the BIOS chip, are tagged with identification codes so that the system will not boot-up if any component is missing or a substitution has been detected.
4. A firmware 'dongle' is incorporated in the case and includes encryption codes essential for reading hard-disc files, for operating the computer system and for transmitting and interpreting network messages. The dongle is connected to the system bus and battery supply in such a manner that its removal will result in the loss of its data.

The Casino Station

The casino station acts as a file server for the remote player stations and for a display terminal at the gaming table for viewing by the croupier. It incorporates software that allows the croupier to select and initiate the desired game and that interprets data from the croupier and appropriate players to cast dice, shuffle cards, deal cards, accept pack-cuts, card-deals, dice-throws. The croupier

manages each game, designates player's turns and adjudicates player disputes. For this purpose, the croupier has a display terminal that shows the lie of cards as it would normally appear to him/her in a live game. This display is available to all players, as it would be in a live game.

Since the range of game offered will normally be quite limited and little process power is required to translate signals from players and the croupier into the appropriate display, the casino station will not normally require accessible disc drives. Accordingly, all the security measures listed above in respect of the player stations are applicable to the casino station.

However, as a major function of the casino station is to serve as a communications hub for the player stations and the croupier, it will require diagnostic software to trouble-shoot systems and communications faults. This software can be furnished on a portable disc drive or the like that can be plugged into a socket on the casino station. This drive may contain encryption software or firmware identification codes so that no other drive can be used for the same purpose. In addition, it is desirable to ensure that access to the casino station via this drive or via its casing can is only possible by authorised operators who have physical and electronic keys and who are identified biometrically in a similar manner to that described in respect of the players.

While it will be appreciated that the system of the particular example meets the objectives of the invention as outlined above, many variations are possible without departing from the scope of the invention as outlined herein.

Lisa HORTEN and Elik SZEWACH

By their Attorney

Paul A Grant

29 March, 1999

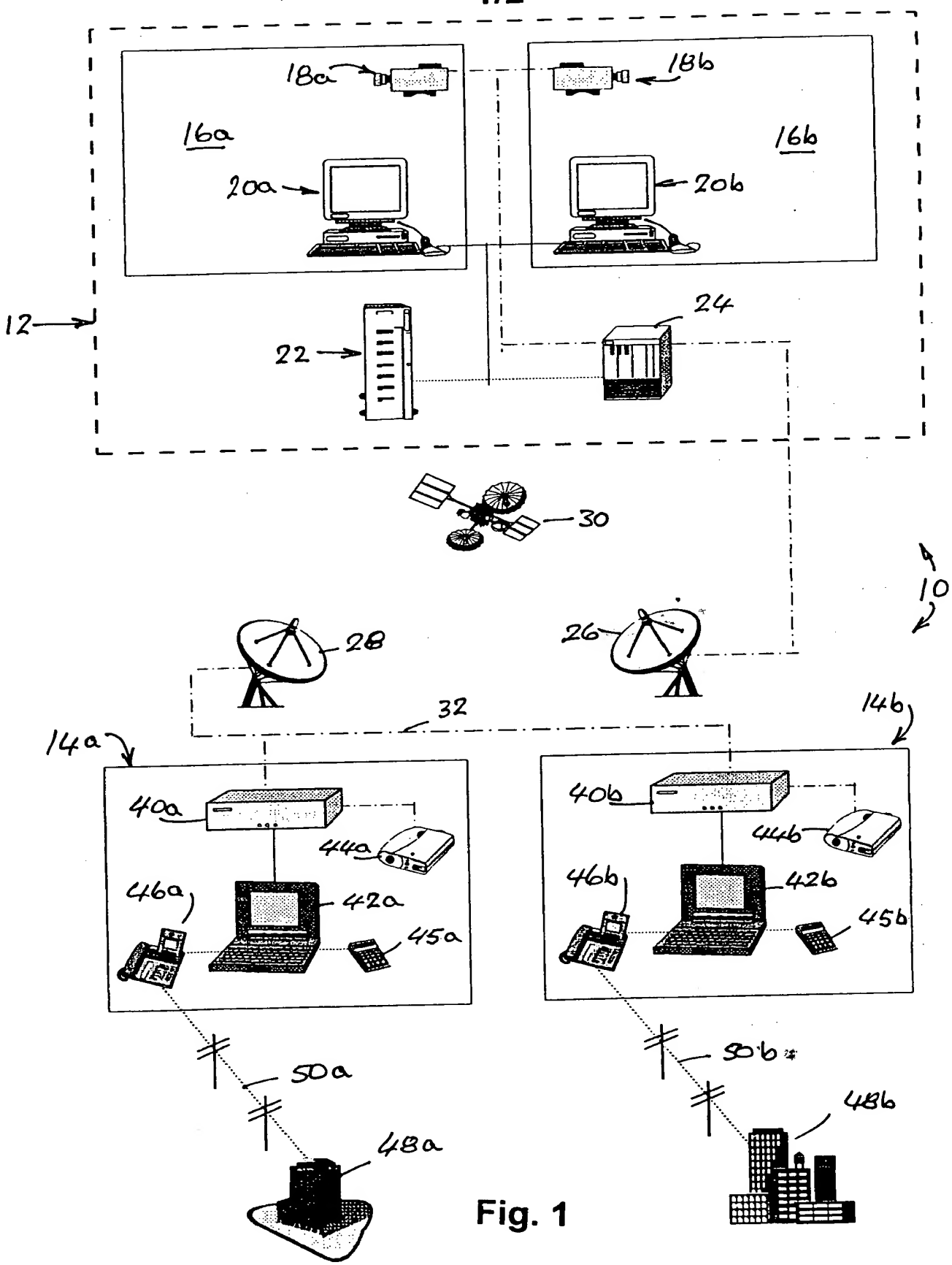


Fig. 1

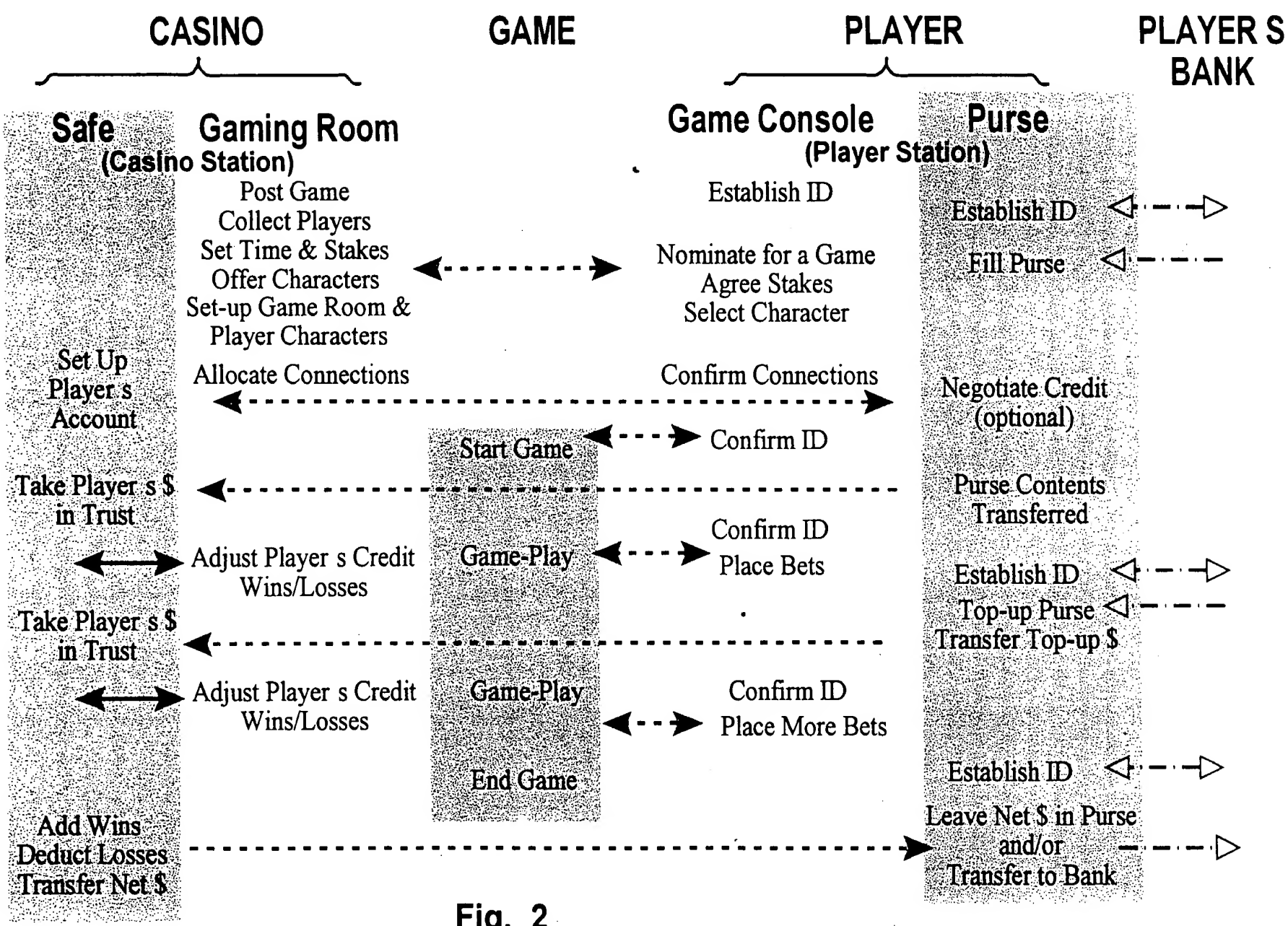


Fig. 2